Network Scanning con Nmap

Josh Van Edward Abanico

7 gennaio 2026

Indice

1 Obiettivo dell'Esercitazione

L'obiettivo di questa attività è l'esecuzione di una scansione di rete approfondita su due target specifici all'interno del laboratorio virtuale:

1. **Target Linux:** Macchina *Metasploitable 2* (Vulnerabile by design).
2. **Target Windows:** Macchina *Windows 10*.

Sono state utilizzate diverse tecniche di scansione offerte dal tool **Nmap** per identificare sistemi operativi, porte aperte e versioni dei servizi, analizzando le differenze tra le metodologie TCP Connect e SYN Scan.

2 Fase 1: Identificazione dei Target

Prima di procedere con le scansioni esterne, è stata verificata la configurazione di rete locale delle macchine target per confermare gli indirizzi IP.

2.1 Identificazione Target Linux (Metasploitable)

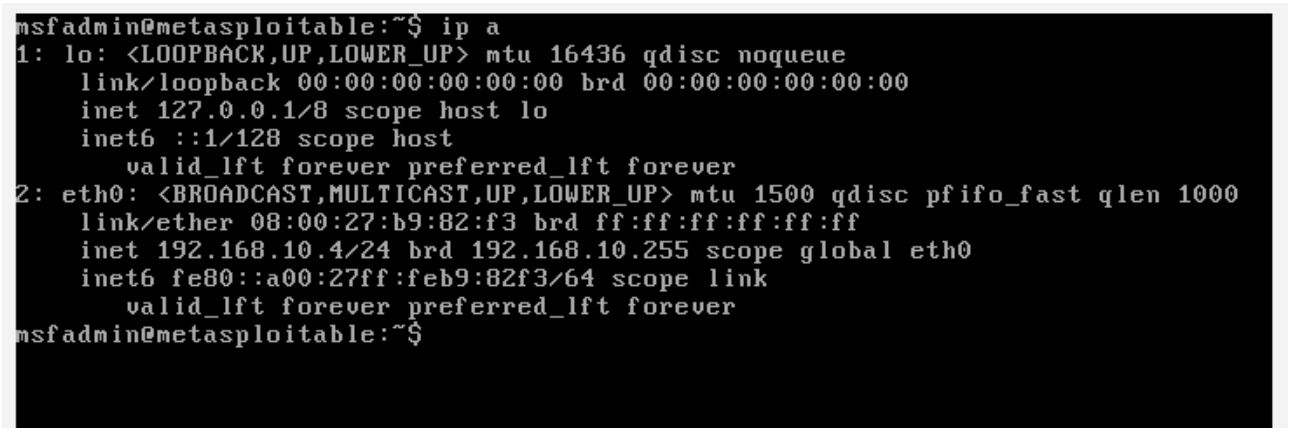

Figura 1: Verifica IP Metasploitable (Command: ip a)

Indirizzo IP rilevato: 192.168.10.4

2.2 Identificazione Target Windows

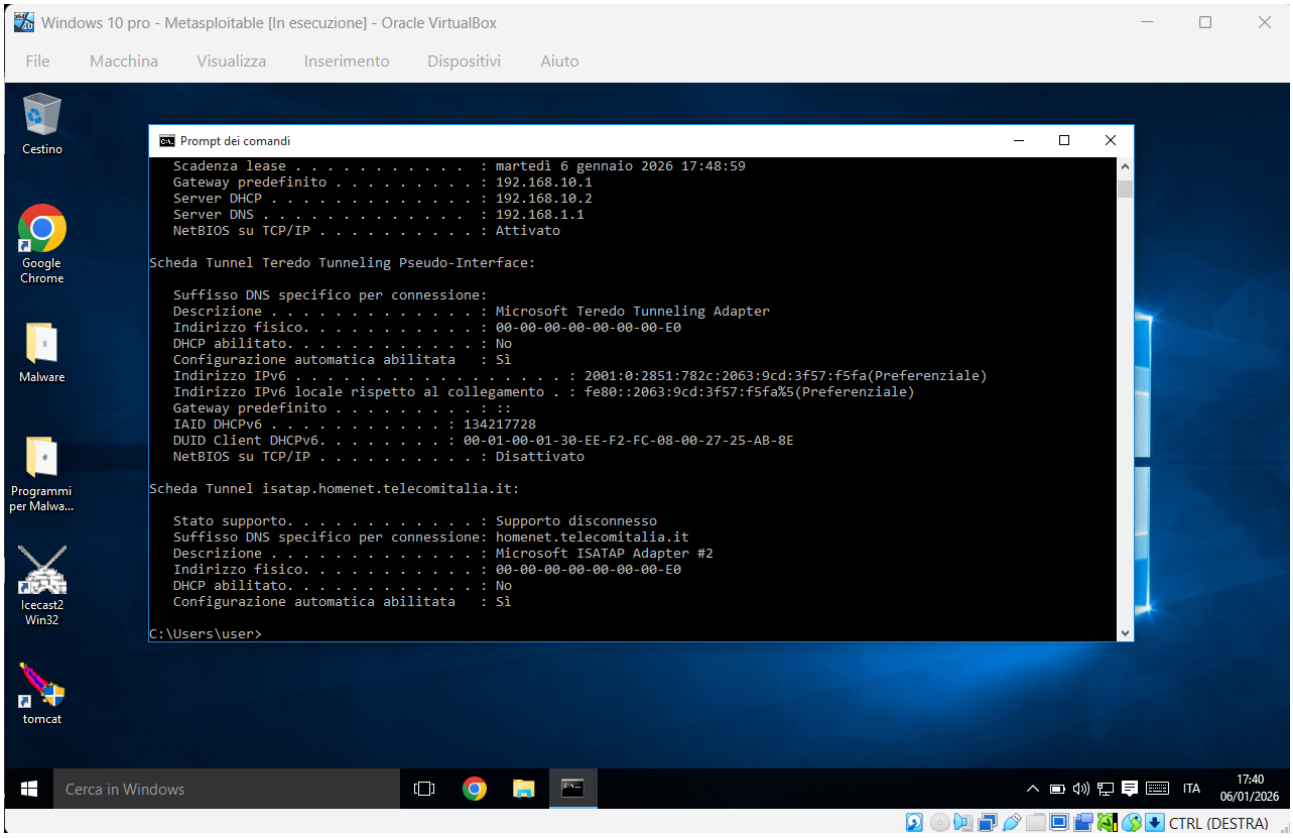

Figura 2: Verifica IP Windows (Command: ipconfig)

Indirizzo IP rilevato: 192.168.10.5

3 Fase 2: Analisi Target Linux (192.168.10.4)

3.1 OS Fingerprinting

È stata eseguita una scansione per identificare il Sistema Operativo sottostante.

```
sudo nmap -O 192.168.10.4
```

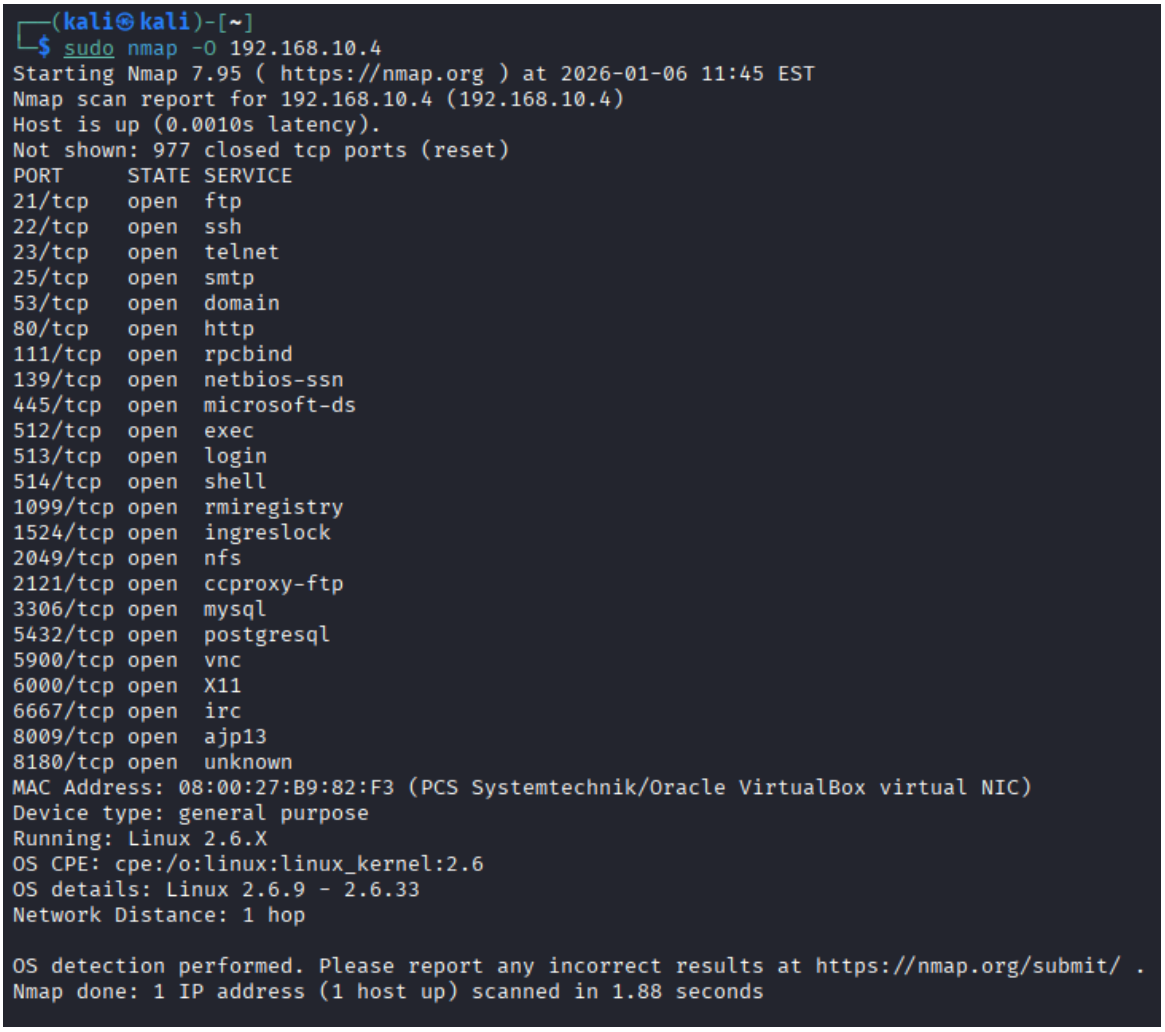

Figura 3: Risultato OS Detection su Metasploitable

Il sistema è stato identificato come Linux, con un kernel compreso tra le versioni 2.6.9 e 2.6.33.

3.2 SYN Scan (Stealth Scan)

Scansione "half-open" eseguita con privilegi di root.

```
sudo nmap -sS 192.168.10.4
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 11:44 EST
Nmap scan report for 192.168.10.4 (192.168.10.4)
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:B9:82:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Figura 4: Risultato SYN Scan (-sS)

La scansione ha rilevato numerose porte aperte (es. 21, 22, 23, 25, 53, 80, 445, 3306) in tempi molto rapidi (0.27 secondi).

3.3 TCP Connect Scan e Confronto

Scansione completa del three-way handshake TCP.

```
sudo nmap -sT 192.168.10.4
```

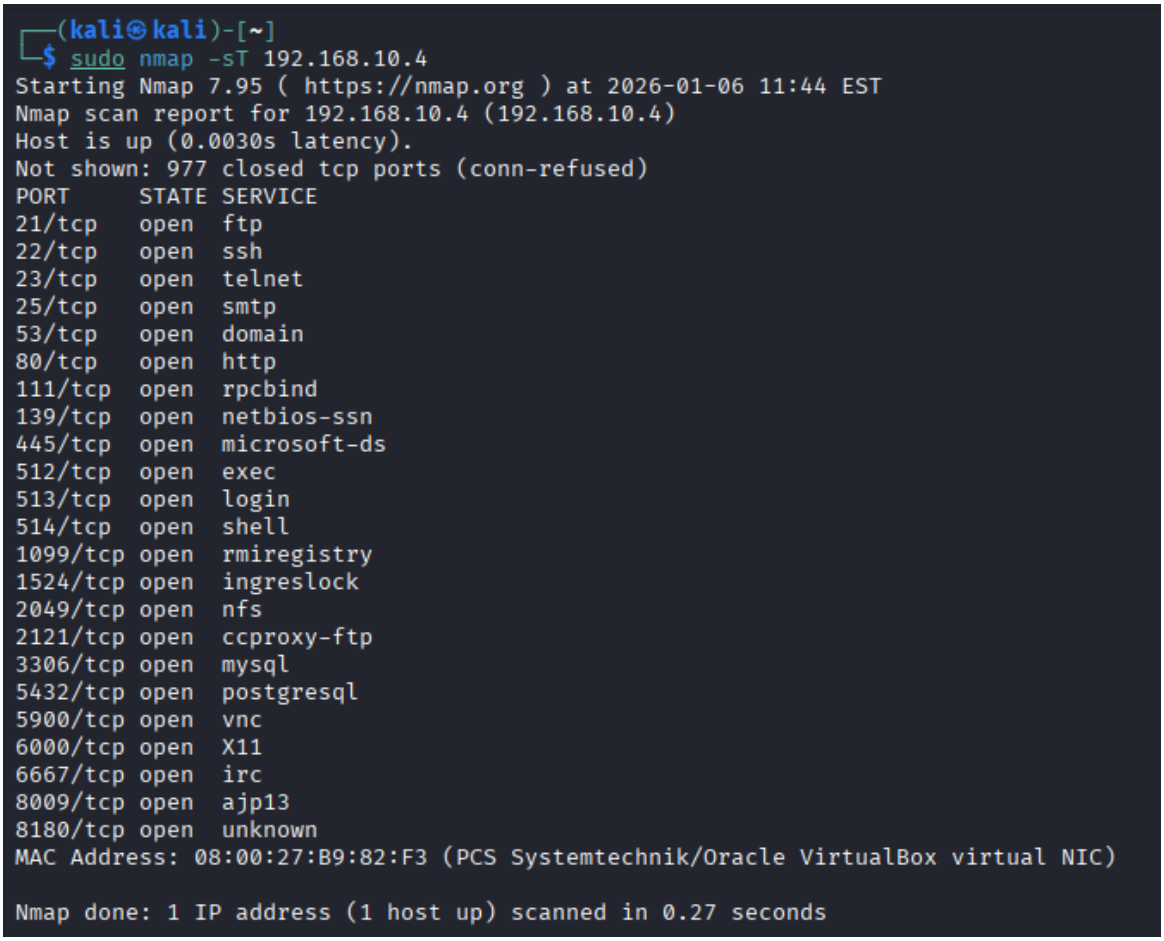

Figura 5: Risultato TCP Connect Scan (-sT)

3.3.1 Differenze Rilevate: SYN vs TCP Connect

Dal confronto degli output (Fig. 4 e Fig. 5):

- **Risultati:** Entrambe le scansioni hanno rilevato le stesse porte aperte.
- **Performance:** La scansione SYN è risultata leggermente più performante in termini di stealth, non completando le connessioni.
- **Comportamento:** La scansione '-sT' stabilisce una connessione completa (SYN → SYN-ACK → ACK), risultando più rumorosa nei log del target rispetto alla '-sS' che invia un RST prima di stabilire la connessione.

3.4 Service Version Detection

Per enumerare le versioni specifiche dei servizi in ascolto.

```
sudo nmap -sV 192.168.10.4
```

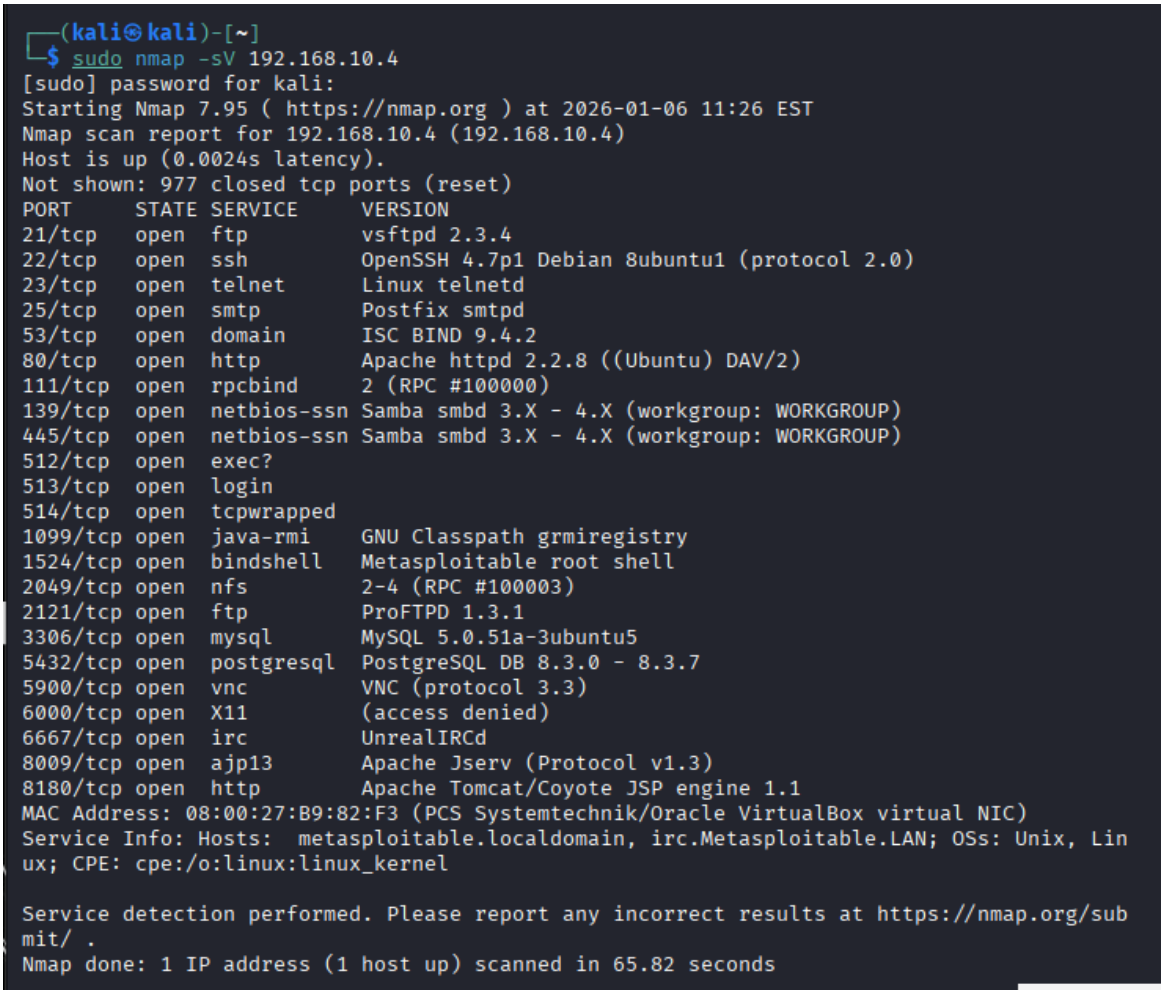

Figura 6: Rilevamento versioni servizi (-sV)

Questa scansione è cruciale in quanto ha esposto versioni software potenzialmente vulnerabili (es. *vsftpd 2.3.4*).

4 Fase 3: Analisi Target Windows (192.168.10.5)

È stata effettuata una scansione combinata per rilevare il sistema operativo e le porte aperte sul secondo target.

```
sudo nmap -O 192.168.10.5
```

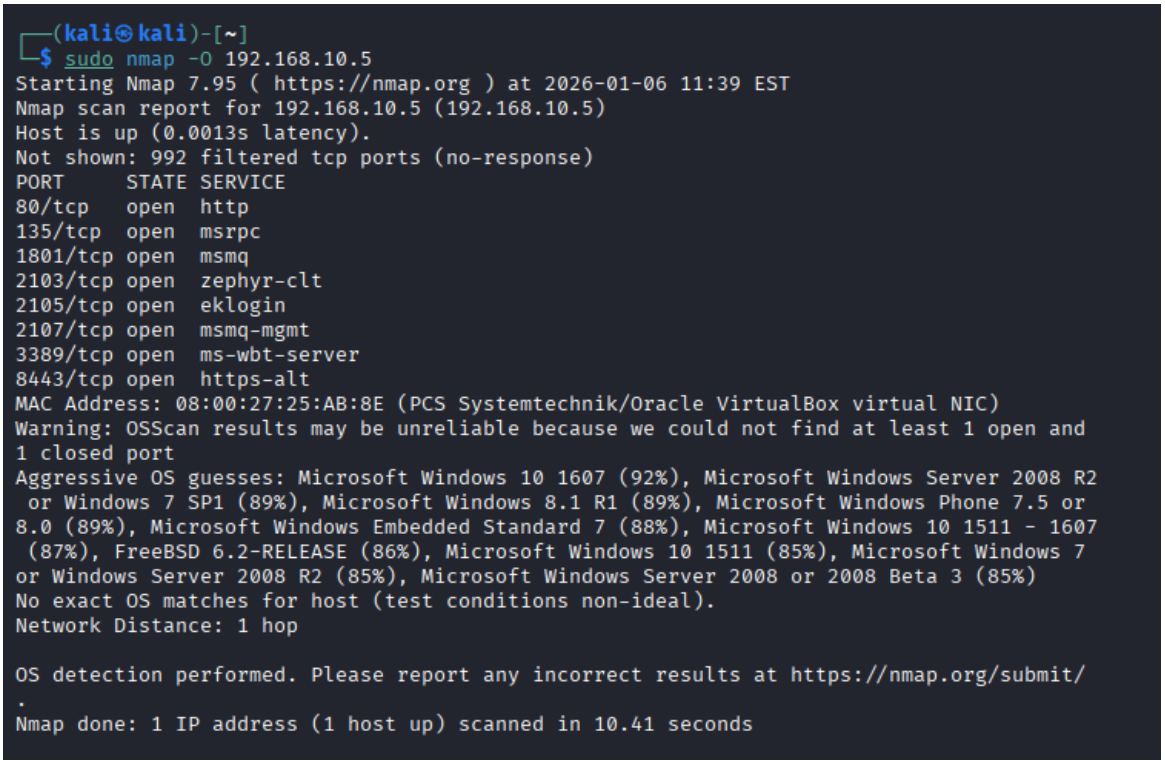

Figura 7: Scansione OS e Porte su Windows

Il target presenta porte tipiche dell'ambiente Windows (135, 3389 RDP) ed è stato identificato con alta probabilità (92%) come Microsoft Windows 10.

5 Conclusioni

L'attività ha permesso di mappare con successo la superficie di attacco di entrambi i target. Mentre la macchina Windows presenta un numero limitato di servizi esposti (principalmente web e RDP), la macchina Linux (Metasploitable) espone un numero elevato di servizi con versioni obsolete (es. vsftpd 2.3.4, Apache 2.2.8).